TAMPEREEN
AMMATTIKORKEAKOULU

EU:n yleisen tietosuoja-asetuksen vaikutus TJB-Yhtiöt Oy:n henkilötietojen käsittelyyn

Sini Lingman

Opinnäytetyö
Toukokuu 2018
Liiketalous
Oikeudellinen asiantuntijuus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden koulutusohjelma
Oikeudellinen asiantuntijuus

LINGMAN, SINI:
EU:n yleisen tietosuoja-asetuksen vaikutus TJB-Yhtiöt Oy:n henkilötietojen käsittelyyn

Opinnäytetyö 41 sivua, joista liitteitä 3 sivua
Toukokuu 2018

Henkilötietojen käsittelyä koskeva lainsäädäntö kokee muutoksen 25.5.2018, kun EU:n yleinen tietosuoja-asetus tulee sovellettavaksi. Asetus tuo yrityksille uusia velvollisuuksia sekä kovempia sanktioita mahdollisista rikkomuksista. Opinnäytetyössä tutkittiin TJB-Yhtiöt Oy:n toimeksiannosta tämän tietosuoja-asetuksen sisältöä ja vaikutuksia yhtiön toimintaan. Toimeksiantajayhtiö toimii teknologia-alalla kahden yrityksen emoyhtiönä hoitaen tytäryhtiöiden henkilöstö- ja taloushallintoa.

Opinnäytetyön tavoitteena oli auttaa toimeksiantajaa kartoittamaan tietosuojakäytänteiden nykytilanne sekä niitä koskevat asetuksen edellyttämät muutokset. Työn tarkoituksena oli tuottaa toimeksiantajalle suositus toimenpiteistä, joiden avulla yhtiö valmistautuu asetukseen. Tämän lisäksi yhtiölle luotiin seloste, jonka avulla yhtiö voi toteuttaa sekä omaa tietosuojapolitiikkaansa että asetuksen edellyttämää osoitusvelvollisuutta. Tutkielma rajattiin käsittelemään pääsääntöisesti toimeksiantajayhtiön kannalta relevantteja asetuksen osioita sekä merkittävimpiä muutoksia. Työssä keskityttiin TJB-Yhtiöt Oy:n tytäryhtiöiden työntekijöiden henkilötietojen käsittelyyn erityisesti palkkatietojen muodossa.

Opinnäytetyön tutkimusmenetelmä oli pääosin lainopillinen. Eri lainopillisia näkökulmia saatiin perehtymällä lainsäädännön lisäksi viranomaisten kirjoittamiin oppaisiin sekä ammattikirjallisuuteen. Lähteiden avulla tietosuoja-asetuksesta pyrittiin saavuttamaan kokonaisvaltainen kuva, jotta johtopäätösten tekeminen helpottuisi. Näin toimeksiantajalle pystyttiin antamaan lainmukaisia ja helposti toteutettavia toimenpide-ehdotuksia.

Lainopillisesta tutkimuksesta selvisi, että asetuksen tuoma sääntely luo merkittävimpiä muutostarpeita yrityksiin, joissa henkilötietoja käsitellään mittavasti. Tutkimus osoitti, että TJB-Yhtiöt Oy:n kannattaa kiinnittää enemmän huomiota tiedon sähköiseen ja fyysiseen suojaamiseen sekä osoitusvelvollisuuden toteuttamiseen. Yksi tutkimuksen keskeisimmistä johtopäätöksistä oli, että tietosuojan huolellisen toteuttamisen tulisi kuulua jokaisen yrityksen tärkeimpiin toimintaperiaatteisiin.

Asiasanat: tietosuoja, yleinen tietosuoja-asetus, henkilötiedot

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration
Option of Legal Expertise

LINGMAN, SINI:
The General Data Protection Regulation and Its Impacts on the Processing of Personal Data at TJB-Yhtiöt Oy

Bachelor's thesis 41 pages, appendices 3 pages
May 2018

The European data protection legislation will go through some significant changes once the General Data Protection Regulation becomes enforceable on 25 May 2018. The regulation sets new responsibilities for companies as well as more severe penalties for breaches. This thesis studies the regulation and its effects on TJB-Yhtiöt Oy, which is a parent company of two subsidiaries in the technology industry.

The objective of this thesis was to study how TJB-Yhtiöt Oy processes their personal data and how their operations are affected by the GDPR. The aim was to give the company a recommendation for actions that would help them prepare for the regulation. In addition, a document was created to indicate that the company's personal data processing is consistent with the regulation. The study was limited to the most relevant issues for the company and it focuses on the personal data such as salary details of the personnel.

This thesis mainly utilised juridical research methods. Along with legislation, the legal aspects were studied in literature and various guide books composed by ministries and other authorities. The use of these diverse sources made it easier to understand the overall procedure that TJB-Yhtiöt should carry out.

The results of the study indicate that the regulation will require notable changes in the companies that process personal data more extensively. The study showed that TJB-Yhtiöt should pay more attention to the protection of physical and digital data and make sure they fulfill their accountabilities. One of the key conclusions of the study was that each company should consider data protection as one of the most important principles in their day-to-day actions.

Key words: data protection, GDPR, personal data

SISÄLLYS

1 JOHDANTO

Yritysten tietosuojakäytännöt kokevat muutoksen keväällä 2018, kun EU:n yleinen tietosuoja-asetus[1] tulee sovellettavaksi. Asetuksen myötä yritysten velvollisuudet henkilötietojen käsittelyssä kasvavat, mikä edellyttää yrityksiltä perehtymistä ja varautumista. Tämä opinnäytetyö toteutetaan toimeksiantona TJB-Yhtiöt Oy:lle, joka resurssien säästämisen vuoksi tarvitsee ulkoisen henkilön selvittämään asetuksen merkitystä. Työssä perehdytään asetukseen ja tietosuojaan sekä yleisellä että yhtiölle konkreettisella tasolla. Opinnäytetyö toteutetaan niin, että sen hyöty toimeksiantajayhtiölle olisi mahdollisimman suuri. Tämän vuoksi työ pyritään pitämään kielellisesti ja sisällöllisesti helppolukuisena ja ymmärrettävänä.

Opinnäytetyön tavoitteena on perehtyä asetuksen sisältöön keskittyen toimeksiantajayhtiön kannalta olennaisimpaan ja mielenkiintoisimpaan sääntelyyn. Tämän lisäksi työssä kartoitetaan yhtiön nykytilanne tietosuoja-asioiden osalta. Työn tarkoituksena on luoda yhtiölle ehdotus toimenpiteistä, joihin heidän kannattaa asetuksen myötä ryhtyä. Työhön liitetään dokumentaatio, jonka avulla yhtiö pystyy suoraan todistamaan henkilötietojen käsittelynsä olevan uuden asetuksen edellyttämällä tasolla. Opinnäytetyö on luonteeltaan pääosin lainopillinen tutkielma, mutta suositukset yhtiön toimenpiteistä muodostetaan pitkälti empiirisesti käyttäen lähteiden lisäksi omia havaintojani. Työssä keskitytään toimeksiantajayhtiössä käsiteltävien tietojen osalta pääsääntöisesti henkilökunnan palkkatietoihin.

Työssä määritellään aluksi muutamia tietosuojaan liittyviä peruskäsitteitä nykylainsäädännön pohjalta, jonka jälkeen ryhdytään avaamaan EU:n yleistä tietosuoja-asetusta. Kuten aiemmin mainittiin, työ rajataan niin, että se sisältää mahdollisimman vähän yhtiön kannalta epäolennaista tietoa. Asetuksen läpikäymisen jälkeen työssä esitellään toimeksiantajayhtiötä ja sen tämänhetkisiä tietosuojakäytäntöjä. Lopuksi esitellään asetuksen vaikutuksia yhtiön toimintaan sekä konkreettisia suosituksia huomiota vaativista toimenpiteistä. Pohdinta -osiossa käydään läpi työn tuloksia ja johtopäätöksiä sekä reflektoidaan omaa työskentelyäni.

---

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti)

Tietosuojalainsäädännön uudistuksesta on tehty paljon tutkimusta, ja yrityksille suunnattuja oppaita löytyy Internetistä lukuisia. Samasta aiheesta on myös kirjoitettu runsaasti opinnäytetöitä viimeisten muutamien vuosien aikana, mutta tämä työ eroaa vastaavista tutkielmista, sillä se räätälöidään kokonaisuutena TJB-Yhtiöt Oy:lle. Työssä käytetään apuna monenlaista aineistoa, kuten lainsäädäntöä, ajankohtaista kirjallisuutta, verkkolähteitä sekä tietenkin itse EU:n asetusta. Kirjallisuudesta tärkeimmäksi teokseksi voidaan mainita Hannisen, Laineen, Rantalan, Rusin ja Varhelan teos Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset, joka ammattitaitoisesti kiteyttää koko asetuksen helposti luettavaan muotoon. Opinnäytetyössä hyödynnetään myös tietosuoja-ammattilaisten luomia oppaita.

Opinnäytetyössä toistuu muutamat olennaiset käsitteet, jotka on hyvä käydä läpi ennen työhön perehtymistä. Rekisterinpitäjällä tarkoitetaan tässä työssä yritystä, joka toiminnallaan päättää, mitä henkilötietoja kerää, ja mihin tarkoitukseen niitä käyttää. Henkilötietojen käsittelijällä taas tarkoitetaan ikään kuin alihankkijaa eli toimijaa, joka käsittelee henkilötietoja rekisterinpitäjän puolesta. (Euroopan komissio) Henkilötietojen käsittelyn kohde on luonnollinen henkilö, jota kutsutaan tässä työssä rekisteröidyksi. Valvontaviranomaisella taas tarkoitetaan kussakin maassa toimivaa viranomaista, joka valvoo asetuksen toteutumista (Tietosuoja-asetus, 51 artikla).

2 TIETOSUOJA YLEISESTI

Tietosuojan voidaan yleisesti katsoa tarkoittavan henkilötietojen käsittelyä, jossa rekisterinpitäjä noudattaa tiettyjä periaatteita rekisteröidyn oikeuksien turvaamiseksi. Tietosuojalla pyritään toteuttamaan henkilötietojen oikeudenmukaista käsittelyä niin, että tiedon kohteen oikeudet ovat aina turvassa. (Andreasson, Koivisto & Ylipartanen 2016, 18.) Tietosuojaa voidaankin tarkastella ikään kuin henkilön immateriaalioikeutena. Andreassonin ym. (2016, 33) mukaan kyse onkin enemmän henkilön itsensä, kuin konkreettisen tiedon suojaamisesta.

Tietosuoja ja tietoturva eivät tarkoita täysin samaa asiaa, vaikka termit monesti saattavatkin mennä sekaisin. Tietoturvalla tarkoitetaan enemmänkin konkreettisia suojaustoimenpiteitä, joita tietosuojan saavuttamiseksi tulee tehdä. Tietoturva voidaan jakaa hallinnollisiin ja teknisiin toimiin. Hallinnollisilla toimilla tarkoitetaan esimerkiksi henkilöstön kouluttamista tai yrityksen toimintalinjauksia, kun taas teknisiin toimiin kuuluvat esimerkiksi järjestelmien suojaaminen viruksilta tai tietoliikenteen reittien valvonta. (Pitkänen, Tiilikka & Warma 2013, 215-216)

Tietoturvallisuus muodostuu pääsääntöisesti tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Tiedon luottamuksellisuus edellyttää, ettei tietoon pääse käsiksi kukaan, kenelle tiedon tutkiminen ei ole oikeutettua. Eheys taas turvaa tiedon muuttumattomana pysymistä eli tiedon tulee säilyä samanlaisena, vaikka ulkoiset olosuhteet pyrkisivät vahingoittamaan tietoa. Tiedon saatavuus taas on ikään kuin tarkennus luottamuksellisuuteen ja sen mukaan tiedon tulee olla siihen oikeutettujen henkilöiden saatavilla. (Pitkänen ym. 2013, 216) Tietoturvallisuuden voidaankin katsoa siis tarkoittavan toimenpiteitä, joita organisaatio tekee saavuttaakseen tiedon luottamuksellisuuden, eheyden ja saatavuuden.

2.1 Henkilötiedot

Suomen perustuslain (731/1999) 10 §:ssä turvataan yksityiselämän suoja, jonka voidaan suurelta osin katsoa koostuvan henkilöä koskevista tiedoista. Henkilötietolaki (523/1999, 3 §) määrittelee henkilötiedon seuraavasti:

> 1) … kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Euroopan unionin tietosuoja-asetuksen määritelmä henkilötiedoista on lähes yksi yhteen yllä olevan kuvauksen kanssa, joskin hieman yksityiskohtaisempi (Oikeusministeriö 2017, 9-10). Henkilötiedon määritelmä on kuitenkin melko kokonaisvaltainen ja sen alle voidaan lukea kaikki henkilöä koskeva yksilöivä tieto riippumatta sisällön totuudenmukaisuudesta tai tiedon muodosta (Pitkänen ym. 2013, 42-43).

Henkilötietojen käsittelyyn sisältyy kaikki henkilötietoihin kohdistuvat toimenpiteet kuten tiedon kerääminen, tallentaminen, suojaaminen tai poistaminen (Henkilötietolaki 523/1999, 3 §). Käsittelyn yleisiä periaatteita ja siihen liittyvää lainsäädäntöä käydään läpi tarkemmin luvussa 3.

2.2 Tietosuoja yrityksissä

Tietosuojatyön merkitys yrityksissä on jatkuvasti kasvussa, ja viimeistään Euroopan unionin yleisen tietosuoja-asetuksen myötä tietosuojaosaaminen nousee yritysten merkittävimpien menestystekijöiden joukkoon. Henkilötietojen hyvin organisoidun käsittelyn voidaankin katsoa mahdollistavan yrityksen menestyksen etenkin digitalisoituvilla markkinoilla. (Andreasson ym. 2016, 17)

Yritysten hallussa on nykypäivänä hyvin paljon henkilötietoja, ja tämän datan säilyttämisen mukana kasvaa myös yritysten vastuu. Jokaisen yrityksen täytyy huolehtia tietosuojan tason ylläpidosta, jotta henkilötietoja ei koskaan väärinkäytettäisi. Mitä enemmän yritys kerää ja käyttää dataa luonnollisista henkilöistä sitä paremmin heidän tulee osata henkilötietojen käsittelyyn liittyvä juridinen tausta (Honkinen, Innanen, Lindgren, Pello, Rantanen, Siltala, Tuomala 2016).

2.2.1 Työntekijöitä koskevat henkilötiedot

Olennainen osa yrityksen henkilötietojen käsittelyä koostuu yrityksen oman henkilökunnan tiedoista. Laki yksityisyyden suojasta työelämässä (759/2004, 3 §) asettaa raamit niille tiedoille, joita työnantaja saa työntekijöistään käsitellä. Lain mukaan sallittua on käsitellä vain henkilötietoja, jotka ovat työsuhteen kannalta tarpeellisia. Tarpeellisuuden käsite ei tässä tapauksessa tosin ole täysin yksiselitteinen, mutta esimerkiksi Nyyssölä (2017) jaottelee työnantajan keräämät tiedot henkilökohtaisiin ja työsuhteessa syntyviin tietoihin.

Nyyssölän (2017) esittämän jaottelun mukaan henkilökohtaisia tietoja ovat muun muassa työntekijän perhe- ja osoitetiedot sekä tiedot aiemmista koulutuksista ja työsuhteista. Työsuhteesta johtuviin tietoihin voidaan taas lukea esimerkiksi tiedot palkasta, terveystarkastuksista ja työsopimuksesta. Lähtökohtaisesti rekisterinpitäjän eli työnantajan vastuulla on selvittää, onko kerätty tai säilytetty tieto tarpeellista, jotta työntekijän oikeuksia tai tietosuojalainsäädäntöä ei rikota.

2.2.2 Pk-yritysten erityishaasteet

Pienissä ja keskisuurissa yrityksissä resurssit ovat monesti tarkkaan mietittyjä, eikä tietoturvan suunnitteluun löydy välttämättä tarvittavaa aikaa ja henkilöstöä. Vuonna 2017 tehdyn vakuutusyhtiö If:n toteuttaman kyselyn mukaan huomattava osa pk-yrityksistä ei ole tarpeeksi varautunut tietoturvariskeihin, eikä ole tietoinen EU:n tietosuoja-asetuksen voimaantulosta (Elo 2017, Kauppalehti). Tietosuoja-asioiden laiminlyönnissä pienikin yritys asettaa itsensä alttiiksi suurille riskeille, joiden toteutuessa tietoturvallisuuden jälleenrakentaminen saattaa viedä yritykseltä merkittävästi rahaa ja aikaa.

Kauppalehden artikkelin (Elo 2017) esittämän tietoturvakyselyn tuloksien mukaan kolmannes pk-yrityksistä on joutunut tietoturvahyökkäyksen kohteeksi viimeisen kolmen vuoden aikana. Näiden rikosten määrän voi odottaa vain kasvavan tulevaisuudessa, joten pienten yritysten on hyvä perehtyä uhkien minimointiin tarpeeksi ajoissa.

3 EU:N YLEINEN TIETOSUOJA-ASETUS

Euroopan unionin yleinen tietosuoja-asetus (General Data Protection Regulation, jatkossa GDPR) vahvistaa lainsäädäntöön säännöt henkilötietojen käsittelylle ja liikkuvuudelle turvaten luonnollisten henkilöiden suojelun. Asetus sisältää 99 artiklaa, jotka voimaantultuaan kumoavat aiemman henkilötietojen käsittelyä koskevan direktiivin 95/46/EY. Suomen kansallisesta lainsäädännöstä asetus kumoaa henkilötietolain (523/1999), jonka tilalle hallitus on esittänyt uuden tietosuojalain säätämistä täsmentämään EU:n asetusta (Oikeusministeriö 2018). GDPR on astunut voimaan 24. toukokuuta 2016 ja se tulee suoraan sovellettavaksi siirtymäajan jälkeen 25. toukokuuta 2018 (OM 2017, 9).

GDPR:n tarkoituksena on tuoda henkilötietojen suojaa ajan tasalle, jotta tietosuojaa koskeviin haasteisiin voidaan reagoida jatkuvasti digitalisoituvassa ja globalisoituvassa maailmassa. Asetuksen tavoitteena on tuoda henkilötietojen käsittelyyn lisää avoimuutta ja tätä kautta turvata rekisteröityjen oikeuksia. (OM 2017, 9) Asetus koskee nimenomaan organisaatioissa tapahtuvaa henkilötietojen käsittelyä ja sisältää tiukempia seuraamuksia säädösten laiminlyönneille, minkä vuoksi yrityksiä on kannustettu päivittämään käytäntönsä asetuksen tasolle jo hyvissä ajoin.

KUVIO 1: Asetuksen sisältö ja tavoite. (OpiTietosuojaa 2017)

OpiTietosuojaa (2017) on tiivistänyt GDPR:n ytimen kuvioon, josta tulee ilmi asetuksen pääsääntöiset tavoitteet ja niiden saavuttamiseen vaadittavat vaiheet. Asetuksen sisältämien oikeuksien ja velvoitteiden kautta saadaan aikaiseksi koko EU:n kattava yhtenäinen tietosuojakäytäntö, mikä mahdollistaa digitaalisten markkinoiden kehittymisen huippuunsa. Tämä edellyttää, että jäsenvaltiot ja organisaatiot toteuttavat asetuksen mukaisesti tietosuojaa heti asetuksen tultua sovellettavaksi.

Asetus sisältää laaja-alaisesti sääntelyä liittyen rekisterinpitäjään, rekisteröityyn, henkilötietojen käsittelijään ja yleisesti henkilötietojen käsittelyä koskeviin toimenpiteisiin. Tässä osiossa käsitellään työn toimeksiantajayhtiön kannalta olennaisia osia asetuksesta aloittaen tietosuojalainsäädännön lähihistoriasta. Asetusta tarkastellaan pääsääntöisesti työnantajan (rekisterinpitäjä) sekä työntekijän (rekisteröity) näkökulmista, jotta hyöty toimeksiantajayritykselle olisi mahdollisimman suuri.

3.1 Lainsäädännön taustaa

Luonnollisen henkilön oikeutta suojella omia tietojaan on turvattu vuosien saatossa useassa kansainvälisessä sopimuksessa. Tämän tietosuojakehityksen voidaan katsoa lähteneen liikkeelle vuosien 1973 ja 1974 Euroopan neuvoston ministerikomitean julkilausumien jälkeen (Vanto 2011, 13). Kansalliseen lainsäädäntöön henkilötietoasiat päätyivät vasta vuonna 1987, kun henkilörekisterilaki säädettiin. Henkilörekisterilaki (471/1987) kumottiin lopulta henkilötietolailla (523/1999) (Vanto 2011, 17). Henkilötietolakia sovelletaan sellaisenaan GDPR:n tuloon 25.5.2018 asti.

Lähiaikojen kehitys EU:n tietosuojauudistusta kohti sai alkusysäyksen tammikuussa 2012, kun Euroopan komissio julkaisi ehdotuksen kyseisen lainsäädännön uudistamisesta. Uudistuksesta, joka sisältää asetuksen lisäksi myös direktiivin lainvalvonnassa käsitellyistä henkilötiedoista, päästiin sopuun joulukuussa 2015 ja säädökset saatiin vakiinnutettua. (Valtiovarainministeriö 2016, 6)

EU:n tällä hetkellä voimassa oleva direktiivi henkilötietojen käsittelystä on annettu vuonna 1995. Tämän jälkeen on tapahtunut paljon muutoksia luonnollisten henkilöiden

tietoturvassa, sillä organisaatioiden toiminta on muuttunut huomattavasti kansainvälisemmäksi ja digitaalisemmaksi viimeisen kahdenkymmenen vuoden aikana. VAHTI-raportin (VM 2016, 6) mukaan tarve riskilähtöisempään sääntelyyn, joka ottaa huomioon uuden teknologian, oli yksi suurimmista tekijöistä GDPR:n muodostumisessa. Yhteiskunnan ja organisaatioiden toiminnan kehitys siis ikään kuin pakotti EU:n reagoimaan kasvaneisiin tietosuojariskeihin. EU jatkaa tätä kehitystä varmasti tulevaisuudessa ja lähiaikojen suunnitelmissa onkin uudistaa myös sähköisen viestinnän tietosuojadirektiivi (VM 2016, 8).

3.2 Asetus rekisterinpitäjän näkökulmasta

Työnantajayrityksen kannalta asetus tuo jonkin verran muutoksia tietosuojakäytäntöihin ja etenkin tarve asioiden tietoisuudesta lisääntyy. Useimmissa tapauksissa yrityksen voidaan katsoa olevan rekisterinpitäjä, mutta on myös olemassa tilanteita, joissa henkilötietojen käsittely on luonteeltaan sellaista, että yritys nähdään erillisenä henkilötietojen käsittelijänä. Tällöin velvollisuudet eroavat hieman. Asetus onkin kohdistanut vaatimuksia edellisestä sääntelystä poiketen suoraan henkilötietojen käsittelijälle (VM 2016, 18).

Suurilta osin asetuksen säädökset ovat vastaavia, kuin aiemmassa kansallisessa lainsäädännössä. GDPR:n periaatteet, kuten luonnollisen henkilön suojaaminen ja jokaisen oikeus omien tietojensa suojaan ovat sellaisenaan löytyneet Suomen lainsäädännöstä jo vuosia (Hanninen ym. 2017, 15). Tästä huolimatta asetuksen säädöksiä on hyvä tarkastella ikään kuin kokonaan uutena sääntelynä, jotta tietosuojalainsäädännön päivittynyt kokonaisuus hahmottuu paremmin. Asetuksen kokonaisvaltainen käyttöönotto on tärkeää etenkin yrityksissä, joissa tietosuoja-asioita ei ole aiemmin juurikaan huomioitu.

3.2.1 Erityisvelvollisuudet

Rekisterinpitäjän vastuulla on huolehtia siitä, että henkilötietoja käsitellään lainmukaisesti. Tietojenkäsittelyn tulee olla huolellista, läpinäkyvää ja aina sidottuna käyttötarkoitukseen (GDPR, 5 artikla). Yrityksen on siis varmistettava, että tarvittavat toimenpiteet suoritetaan, jotta vain tarpeellisia tietoja säilytetään turvallisesti. Rekisterinpitäjän vas-

tuulle jää myös tietosuojan suunnittelu riskeihin suhteutettuna. Mikäli yrityksen henkilötietoja käyttää erillinen henkilötietojen käsittelijä, yritys on itse vastuussa käsittelijän toiminnan lainmukaisuudesta (Hanninen ym. 2017, 26).

Henkilötietojen käsittelijän velvollisuuksista tärkeimpänä voidaan mainita se, että tietojenkäsittely pysyy lain asettamien rajojen sisällä. Yleensä henkilötietojen käsittelijällä on sopimus rekisterinpitäjän kanssa, ja mikäli toiminnan rajat ylittyvät, tämä sopimus rikkoutuu ja henkilötietojen käsittelijää tulee koskemaan sama sääntely, kuin rekisterinpitäjää. (Hanninen ym. 2017, 27) Tällainen tilanne voisi tulla eteen esimerkiksi, jos henkilötietojen käsittelijä käyttäisi rekisterinpitäjän luovuttamia tietoja oman toimintansa edistämiseen, eikä vain ennalta sovitulla tavalla.

3.2.2 Ilmoitus- ja osoittamisvelvollisuus

Asetuksen myötä rekisterinpitäjän ilmoitus- ja osoittamisvelvollisuus kasvaa. Ensinnäkin rekisterinpitäjän tulee ylläpitää selostetta tietosuojatoiminnasta. Tämän selosteen tulee sisältää tiedot yrityksen vastuulla olevista henkilötiedoista sekä niiden käsittelytoiminnoista (GDPR, 30 artikla). Mitä tarkempi tämä seloste on, sitä varmemmin yritys pysyy itse tietoisena toiminnastaan sekä pystyy tarpeen tullen osoittamaan nopeasti toimintansa lainmukaisuuden. VAHTI-raportin (2016, 27) mukaan tämä dokumentaatio toimii samalla myös tietosuojapolitiikkana, jonka mukaisesti yritys toimii. Näin koko organisaatio tietää, miten tietosuoja-asioita hoidetaan ja miten niitä tulee myös jatkossa hoitaa.

Mikäli yritys haluaa vahvasti osoittaa noudattavansa tietosuoja-asetusta, on sen mahdollista saada itselleen tietosuojasertifikaatti. Sertifioinnin voi saada sen myöntämiseen pätevältä sertifiointielimeltä, mutta asetuksen 42 artiklan mukaan sellaisen saadessaan vastuu asetuksen noudattamisesta pysyy silti samanlaisena. Sertifioinnin tuoma todistus ei siis välttämättä yksinään riitä, vaan tietosuojakäytänteitä tulee jatkuvasti ylläpitää asetuksen mukaisina. Yrityksissä, joissa henkilötietojen käsittely on vähäistä, pysyy osoittamisvelvollisuus varmasti yllä yrityksen itse laatiman selosteen avulla.

Näiden osoittamisvelvollisuuksien lisäksi asetus suojaa tietojen turvallisuutta myös ilmoitusvelvollisuudella. Tämä tarkoittaa sitä, että riskialttiiden tietojen tietoturvalouk-

kauksen sattuessa rekisterinpitäjän on 72 tunnin kuluessa ilmoitettava valvontaviranomaiselle ja kerrottava, mitä on tapahtunut ja millaisia seurauksia tapahtuneella mahdollisesti on. (GDPR, 33 artikla) Säädöksen merkitys on tärkeä etenkin arkaluonteista tietoa käsitteleville yrityksille, sillä mitä nopeammin tietoturvaloukkaukseen reagoidaan, sitä nopeammin saadaan korjattua rekisteröidylle koituvia vahinkoja. Valvontaviranomaisen lisäksi rekisterinpitäjän tulee ilmoittaa myös rekisteröidylle tällaisesta loukkauksesta. Hannisen ym. (2017, 111) mukaan kynnys on korkeampi rekisteröidylle ilmoitettaessa. Tämä tarkoittaa sitä, että tilanteissa, joissa loukkaus aiheuttaa suuren riskin rekisteröidyn henkilökohtaisten tietojen vuotamiselle, tulee rekisterinpitäjän ilmoittaa rekisteröidylle tapahtuneesta. Ilmoitusvelvollisuuden tärkeydestä voidaan päätellä, että tietosuojaloukkauksiin reagoimisen tulee aina olla nopeaa, vaikka loukatut tiedot eivät laatunsa vuoksi aina vaatisikaan valvontaviranomaisen yhteydenottoa.

3.2.3 Tietojenkäsittelysopimus

Tietosuoja-asetuksen edellytyksien mukaan kaikissa tilanteissa, joissa rekisterinpitäjän puolesta henkilötietoja käsittelee erillinen henkilötietojen käsittelijä, tulee asiasta laatia tietojenkäsittelysopimus (Hanninen ym. 2017, 82). Tällaisella sopimuksella saadaan kummankin osapuolen oikeudet ja velvollisuudet esille, jotta molemmille puolille on selvää, millaisia tietoja saa käsitellä ja miten. Yleinen tilanne yrityksille tietojenkäsittelysopimuksen vaativasta suhteesta on kirjanpidon tai palkanlaskennan ulkoistaminen. Näissä tapauksissa yritys toimii rekisterinpitäjänä, ja henkilötietojen käsittelijänä toimii esimerkiksi palkanlaskija, joka tarvitsee yrityksen henkilötietoja voidakseen käsitellä niitä yrityksen puolesta.

Tietojenkäsittelysopimus tulee GDPR:n myötä laajemmin käytettäväksi, sillä tämä selkiyttää rekisterinpitäjän ja henkilötietojen käsittelijän suhdetta. Myös osapuolten oikeusturvan kannalta on hyvä, että tietojenkäsittelysopimukset tehdään huolellisesti, sillä niistä käy ilmi esimerkiksi salassapitovelvollisuuden ulottuvuus. VAHTI-raportin (VM 2016, 29) ohjenuorien mukaan sopimusten toteutumista tulee seurata sekä sisältöä päivittää, mikäli henkilötietojen sisältö muuttuu esimerkiksi riskiluonteisemmaksi.

3.2.4 Riskienhallinta

GDPR perustuu riskilähtöiseen lähestymistapaan, joten yrityksen tulee mitoittaa tietosuojatoimenpiteensä rekisteröidylle aiheutuviin riskeihin (Andreasson, Riikonen & Ylipartanen 2017, 30). Tämä tarkoittaa käytännössä sitä, että vaikka yrityksen tulee suojata tunnistettavissa olevaa tietoa, ei ole kannattavaa ylimitoittaa toimenpiteitä tilanteissa, joissa riskit ovat matalia. Toisaalta taas rekisteröidyn oikeuksiin kohdistuvien riskien ollessa korkeita, on oletettua, että tietoturvaloukkauksiin varaudutaan hyvinkin mittavasti.

Tietosuojariskien analysointi tulee varmasti viimeistään asetuksen myötä ajankohtaiseksi jokaisessa organisaatiossa. Tämän lisäksi GDPR määrää 35 artiklassa, että tilanteissa, joissa toimenpiteet aiheuttavat todennäköisen riskin luonnollisen henkilön oikeuksien ja vapauksien kannalta, tulee tehdä niin kutsuttu vaikutustenarviointi. Esimerkiksi uuden teknologisen tiedonsäilytysjärjestelmän käyttöönotto saattaisi edellyttää vaikutustenarvioinnin toteuttamista. Tällaisessa tilanteessa ei voitaisi olla varmoja siitä, säilyykö tieto koko prosessin ajan turvassa, joten järjestelmän tietoturvallisuutta tulisi arvioida tarkemmin. Vaikka vaikutustenarviointi on pakollista vain tilanteissa, joissa riski on suuri, on henkilötietoja käsittelevän yrityksen aina tarpeen ottaa riskit huomioon suunniteltaessa uutta toimintoa, joka sisältää henkilötietojen käsittelyä.

3.2.5 Tietoturvallisuuden takaaminen

Rekisterinpitäjän tulee, käsittelyn laajuus ja riskit huomioon ottaen, toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, jotta henkilötietojen käsittelyn turvallisuus olisi kyseiselle organisaatiolle vastaavalla tasolla. Tämän tason saavuttamisen keinoiksi voidaan lukea esimerkiksi rekisteröidyn tunnistettavuuden poistaminen eli pseudonymisointi, tietoturvallisuuden perusperiaatteiden toteuttaminen sekä nopea reagointi muuttuviin tilanteisiin. (GDPR, 4 & 32 artikla) Näissäkin toimenpiteissä yrityksen tulee muistaa suhteuttaa toiminta tietojen laatuun ja riskin laajuuteen. VAHTI-raportin (VM 2016, 24) mukaan rekisterinpitäjän tulee pitää huolta tietoturvallisuudesta usealla eri osa-alueella tiedon keräämisestä sen hävittämiseen asti. Näin ollen tietoturvallisuuteen kuuluu tiedon oikean säilyttämisen lisäksi myös sen oikea-aikainen ja -tapainen hävitys.

GDPR lisää 32 artiklassa tietoturvallisuuden perusperiaatteisiin (luottamuksellisuus, eheys ja saatavuus) myös vikasietoisuuden. Tämä tarkoittaa sitä, että tekninen laite kestää mahdollisen vian ilman, että henkilötietojen suoja kärsii. Sähköisten järjestelmien lisääntyessä jatkuvasti, on entistä tärkeämpää, että tiedot ovat tallennettuina kestäviin ja luotettaviin järjestelmiin. Hannisen ym. (2017, 109) mukaan yrityksen tulisi säännöllisesti tutkia henkilötietoja sisältäviä järjestelmiä, jotta voidaan minimoida kaikki tiedon väärinkäytökset.

3.2.6 Tietosuojavastaava

EU:n tietosuoja-asetuksen 37 artiklassa on määritelty tilanteet, joissa organisaation tulee nimittää tietosuoja-asioiden hoitoon erillinen tietosuojavastaava. Tietosuojavastaava on pakko nimittää tilanteessa, jossa tietojenkäsittely tapahtuu viranomaisen toimesta tai, jossa rekisterinpitäjän toiminta muodostuu pääosin laajamittaisesta rekisteröityjen seuraamisesta etenkin, jos tämä laajamittainen käsittely kohdistuu rikostietoihin tai erityishenkilöryhmiin. Käytännössä siis tietosuojavastaavan pakollinen nimittäminen kohdistuu lähinnä julkiseen sektoriin eli se ei koske yrityksiä, joissa käsiteltävät henkilötiedot ovat ns. tavanomaisia asiakas- tai henkilöstötietoja.

Tietosuojavastaavan työnkuvaan kuuluu noudattaa ja panna täytäntöön GDPR:n mukaista tietosuojatoimintaa sekä neuvoa ja ohjata organisaatiota. Tämän lisäksi tietosuojavastaava toimii yhteistyössä valvontaviranomaisen kanssa ja mahdollisesti on vastuussa ilmoitusvelvollisuuden toteuttamisesta. (Andreasson ym. 2017, 86-87) Vaikka varsinaisen tietosuojavastaavan nimittäminen ei ole tarpeellista suurimmassa osassa yksityisen sektorin yrityksistä, on rekisterinpitäjän silti aina hyvä delegoida tietoturva-asioiden hoito yhdelle tai muutamille ihmisille. Tällaisen pienimuotoisen tietosuojaorganisaation muodostaminen helpottaa tilanteissa, joissa tietosuoja-asiat tulevat eteen, esimerkiksi uuden asetuksen tuovan osoittamisvelvollisuuden kanssa (VM 2016, 20)

3.2.7 Sanktiot rikkeistä

Yritysten kannalta ehkäpä merkittävin muutos EU:n yleisessä tietosuoja-asetuksessa on tapahtunut seuraamusjärjestelmässä. Aiemmin henkilötietolaissa (523/1999 47 § ja 48 §) seuraamukset käsiteltiin oikeastaan joko vahingonkorvauslain (412/1974) tai rikoslain

(39/1889) perusteella. Uuden asetuksen 83 artiklan mukaan valvontaviranomainen voi määrätä yritykselle hallinnollisia sakkoja, mikäli yritys laiminlyö asetusta tietosuojatoiminnassaan. Vahingonkorvausvelvollisuus säilyy tietosuojarikkeissä edelleen, mutta rikosoikeudellinen vastuu rajoittuu kaksoisrangaistavuuden kiellon vuoksi koskemaan vain niitä tilanteita, joissa hallinnollista sakkoa ei anneta (Oikeusministeriö: TATTI 2017, 110). Sakkojen tuominen lainsäädäntöön toimii varmasti varoittavana ja jopa uhkaavana keinona ja saa yritykset miettimään tietoturvallisuuttaan hieman tarkemmin.

Hallinnollisten sakkojen enimmäismäärään vaikuttaa se, kuinka perustavanlaatuista velvoitteiden rikkominen on ollut. Rikkeen voidaan katsoa olleen perustavanlaatuinen, mikäli se rikkoo asetuksen perusperiaatteita, jotka ovat mainittu artikloissa 5, 6, 7 ja 9. (GDPR, 83 artikla) Näihin perusperiaatteisiin lukeutuu muun muassa tietojenkäsittelyn lainmukaisuus, rekisteröidyn suostumus sekä arkaluonteisten tietojen käsittely. Myös rekisteröidyn oikeuksiin sekä EU:n ulkopuolisiin siirtoihin kohdistuvia rikkomuksia voidaan pitää perustavanlaatuisina. Näistä rikkomuksista seuraava hallinnollinen sakko on enintään 20 miljoonaa euroa tai 4 prosenttia yrityksen liikevaihdosta, riippuen siitä kumpi on suurempi. Muiden säännösten laiminlyönnistä voi saada hallinnollisen sakon, jonka suuruus on enintään 10 miljoonaa euroa tai 2 prosenttia liikevaihdosta. (GDPR, 83 artikla)

Jokainen tietosuojaa koskeva tilanne arvioidaan yksilöllisesti, ja valvontaviranomaisen tulee punnita tapahtunutta rikkomusta esimerkiksi sen perusteella, kuinka laajasti tilanne vaikuttaa rekisteröityihin tai miten yritys on toiminut rikkomisen jälkeen (Hanninen ym. 2017, 129). Todennäköistä ei ole, että viranomaiset kiertäisivät jokaisen yrityksen läpi ja antaisivat miljoonien sakkoja pienimmistäkin puutteista. Enimmäissummat ovat kuitenkin sen verran suuria, että etenkin pk-yritysten talous voi horjahtaa sakkorangaistuksesta tuntuvasti. Tästä syystä yritysten kannattaa pienilläkin toimenpiteillä yhdenmukaistaa toimintansa GDPR:n kanssa.

3.3 Asetus rekisteröidyn näkökulmasta

EU:n tietosuoja-asetus sisältää yksityiskohtaisia säädöksiä rekisteröidyn oikeuksista tietojensa turvaamiseksi. Nämä oikeudet voidaan nähdä samalla myös rekisterinpitäjän vel-

vollisuuksina, sillä rekisterinpitäjän vastuulla on huolehtia näiden oikeuksien toteutumisesta. Tästä syystä rekisteröidyn oikeuksien rikkominen kuuluukin rikkeisiin, joista voi saada suurimmat hallinnolliset sakot. Suurilta osin asetuksen sääntelemät rekisteröidyn oikeudet ovat vastaavia, kuin henkilötietolaissa, mutta joitakin oikeuksia asetus tuo myös uutena lainsäädäntöön (VM 2016, 13). Yksityiskohtaisten säädösten tarkoituksena on vahvistaa koko GDPR:n ydintarkoitusta eli luonnollisen henkilön tietojen suojaamista.

3.3.1 Tiedonanto

Aiemmin mainitun rekisterinpitäjän ilmoitusvelvollisuuden lisäksi rekisteröidyllä on oikeus saada tietää henkilötietojen käsittelystä ennen kuin käsittelytoimet aloitetaan. Asetus on tuonut näihin tiedonantovelvoitteen alaisiin asioihin uutena henkilötietojen säilytysajan sekä tietosuojavastaavan yhteystiedot. (VM 2016, 14) Asetuksen 13 ja 14 artiklat erittelevät kaksi eri tilannetta tietojen keräämiselle: tietojen kerääminen rekisteröidyltä itseltään ja tietojen kerääminen muualta. Käytännössä rekisteröidylle toimitettavat tiedot henkilötietojen käsittelystä ovat molemmissa tilanteissa samat, mutta mikäli tietoa kerätään muista lähteistä, tulee rekisteröidylle ilmoittaa myös, mistä ja millaista henkilötietoa on kerätty.

Tiedonantoilmoitukseen sisältyy jo yllämainittujen lisäksi esimerkiksi henkilötietojen käsittelyn tarkoitus, luovutettujen tietojen vastaanottajat ja rekisteröidyn oikeudet tietojensa suhteen (VM 2016, 14). Läpinäkyvyyden kannalta on tärkeää, että rekisteröidyllä on aina saatavilla tieto omien henkilötietojensa käsittelyn perustasta, jotta luottamus rekisterinpitäjään säilyy ja rekisteröidylle jää mahdollisuus kieltäytyä tietojenkäsittelystä. Käytännössä tällaiset sähköiset, aina saatavilla olevat kuvaukset henkilötietojen käsittelystä tulevat sovellukseen yrityksissä, joissa henkilötietoja kerätään paljon tai niitä hyödynnetään monella eri tapaa.

3.3.2 Tietoihin pääsy

Rekisteröidyllä on oikeus rekisterinpitäjältä saatuun vahvistukseen siitä, käsitelläänkö hänen henkilötietojaan yrityksessä. Mikäli yritys käsittelee asiaa tiedustelevan luonnollisen henkilön tietoja, on tällä henkilöllä oikeus nähdä tiedot, joita hänestä säilytetään. Asetuksen 15 artiklassa on lueteltu lisäksi tiedot, jotka rekisteröidyllä on oikeus saada, mikäli

hänen henkilötietojaan käsitellään. Nämä kohdat ovat hyvinkin vastaavat tietoihin, jotka rekisteröidylle tuli ilmoittaa ennen käsittelytoimien aloittamista (3.3.1). Tietojen osoittaminen rekisteröidylle hänen halutessaan on toimenpide, johon jokaisen yrityksen on hyvä varautua. Voidaan kuitenkin päätellä, että yritykset, joiden rekisterissä on esimerkiksi laajamittaisia asiakastietoja, joutuvat varmasti käsittelemään selvityspyyntöjä huomattavasti enemmän kuin yritykset, joissa käsiteltävät henkilötiedot liittyvät vain yrityksen omaan henkilöstöön.

3.3.3 Tietojen oikaisu ja poistaminen

Sen lisäksi, että rekisteröidyllä on oikeus saada tieto häntä koskevasta henkilötietojen käsittelystä, rekisteröidyn on mahdollista vaatia tietojen oikaisua tai niiden poistoa. Hannisen ym. (2017, 61) mukaan rekisteröidyllä on oikeus epätarkan ja virheellisen tiedon korjaamiseen ottaen kuitenkin huomioon tietojen alkuperäisen käsittelyn tarkoituksen. Olennaista yrityksen kannalta on, että tiedot ovat sellaisissa järjestelmissä, joista tietoa pystyy muokkaamaan myös jälkikäteen. Oikaisutapauksissa rekisteröidyn on esitettävä mahdollisesti lisäselvityksiä, mikäli haluaa jonkin henkilötietonsa rekisterinpitäjän järjestelmästä muokatuksi (GDPR, 16 artikla).

Tietojen poistamisesta käytetään myös termiä ”oikeus tulla unohdetuksi”. Karkeasti tulkittuna rekisteröidyllä on oikeus saada tietonsa pyyhittyä pois yrityksen käsittelystä. Tällaiseen vaatimukseen tulee rekisteröidyltä tosin löytyä jokin asetuksessa säännellyistä perusteluista. Lyhyesti sanottuna tietojen poistamiseen riittää perusteluksi esimerkiksi henkilötietojen alkuperäisen tarpeen lakkaaminen, rekisteröidyn suostumuksen purkaminen tai käsittelyn lainvastaisuus (GDPR, 17 artikla). Näin ollen siis rekisteröidyn halu poistaa henkilötietojaan ei voi olla täysin mielivaltaista. On myös tilanteita, joissa jokin edellä mainituista perusteista täyttyy, mutta henkilötietojen käsittelyn peruste on ikään kuin vahvempi tekijä. Tällainen tilanne on esimerkiksi työyhteisössä, jossa työntekijöiden henkilötietojen käsittely on yrityksen etujen toteutumisen kannalta välttämätöntä. Näin ollen työntekijöillä ei lähtökohtaisesti ole oikeutta unohdetuksi tulemiselle. (Hanninen ym. 2017, 63) Mikäli kuitenkin tietojen poistamiselle löytyy perusteet, tulee yrityksen hävittää kyseisen luonnollisen henkilön tiedot kaikista järjestelmistään. Vaikka Hanninen ym. (2017, 63) esittää, että asetuksessa ei oteta kantaa varmuuskopioissa sijaitseviin tietoihin,

on oletettavaa, että henkilötietojen poistaminen koskee kaikkia yrityksen hallussa olevia järjestelmiä ja asiaan liittyviä papereita.

3.3.4 Tietojen siirtäminen

Yksi uusista asetuksen osioista rekisteröidyn oikeuksiin on oikeus siirtää tiedot järjestelmästä toiseen. Tämä tarkoittaa asetuksen 20 artiklan mukaan sitä, että rekisteröidyn on saatava tietonsa rekisterinpitäjältä sellaisessa muodossa, että hänen on mahdollista suoraan siirtää ne toiselle rekisterinpitäjälle. Tiedon siirtäminen kuitenkin edellyttää GDPR:n mukaan sitä, että tiedon tulee olla sellaista, jonka käsittely perustuu rekisteröidyn itsensä suostumukseen. Hannisen ym. (2017, 65) mukaan tilanne voi olla hankala, mikäli tiedon käsittely perustuu sekä rekisteröidyn suostumukseen että yrityksen etuun. Tällainen tilanne on mahdollinen esimerkiksi työntekijää koskevissa tiedoissa, sillä osa tietojenkäsittelystä perustuu rekisteröidyn suostumukseen (työsopimus) ja osa yrityksen edun toteuttamiseen (työsuhteen kannalta olennaiset tiedot). Pääsääntöisesti voidaan kuitenkin todeta, että järjestelmien välisten siirtojen mahdollistamiseen tulee varautua etenkin yrityksissä, joissa laajat asiakasrekisterit esimerkiksi verkkopalveluissa perustuvat sopimukseen (Hanninen ym. 2017, 65). Asetuksen perusteella rekisteröidyn siirto-oikeus ei kuitenkaan varsinaisesti edellytä tavalliselta yritykseltä toimenpiteitä.

3.3.5 Vastustaminen

Henkilökohtaisen tilanteen perusteella rekisteröidyllä on oikeus vastustaa häntä koskevien tietojen käsittelyä, ellei käsittelylle löydy niin tärkeää syytä, että se syrjäyttää rekisteröidyn edun. Näin ollen monet tilastotieteelliset ja julkisen sektorin rekisterit eivät sovellu vastustamisoikeuden toteuttamiseen. Vastaavalla tavalla rekisteröidyllä on asetuksen 21 ja 22 artiklan perusteella oikeus jättäytyä pois sellaisesta automatisoidusta päätöksenteosta, jossa häntä esimerkiksi profiloidaan tietojensa perusteella merkittävällä tavalla. Asetuksessa mainittua profilointia voi olla esimerkiksi sähköinen työpaikkahaku, jossa karsitaan hakijoita jo pelkän sähköisen järjestelmän avulla ilman ihmisten osallistumista. Tällaiset rekisteröidyn vastustamisoikeuksien toteuttamiset todennäköisesti harvoin koskevat pk-yritystä, jonka hallussa on lähinnä tietoa työntekijöistä.

3.4. Kansallinen liikkumavara

Vaikka tietosuoja-asetus tulee sellaisenaan sovellettavaksi Suomen lainsäädäntöön, jättää se jonkin verran liikkumavaraa aiemman tietosuojadirektiivin tapaan. Tämä tarkoittaa käytännössä sitä, että voidaan säätää asetusta tarkentavia lakeja, jotka sääntelevät henkilötietojen käsittelyä jäsenvaltiolle yksilöidyllä tavalla. Lähinnä tätä liikkumavaraa löytyy julkisella sektorilla, mutta jonkin verran myös yksityisellä sektorilla (OM: TATTI 2017, 98). Hallitus on maaliskuussa 2018 luonut eduskunnalle esityksen tietosuoja-asetusta täydentävästä kansallisesta lainsäädännöstä (HE 9/2018). GDPR:n kokonaisuuden ja tulevaisuuden mahdollisten muutosten vuoksi on hyvä jossain määrin olla tietoinen kansallisen liikkumavaran sisällöstä. EU:n tietosuoja-asetuksen täytäntöönpanoryhmä (TATTI) on julkaissut mietinnön, joka sisältää taulukoituna kansallisen liikkumavaran kaikkien asetuksen artikloiden osalta sekä ehdotuksia siitä, miten artiklat otetaan huomioon lainsäädännössä. Tässä osiossa käsitellään pintapuolisesti asetuksen jättämää liikkumavaraa kansalliseen lainsäädäntöön.

TATTI-työryhmä (OM 2017, 48) jaottelee artikloita viidellä kriteerillä: ei kansallista liikkumavaraa, huomioitava, mahdollisuus, velvollisuus ja notifiointivelvollisuus Euroopan komissiolle. Asetuksessa kansallista liikkumavaraa ei jää esimerkiksi rekisterinpitäjän vastuuseen eikä useimpiin EU:n ulkopuolelle tapahtuviin tiedonsiirtoihin. Lisäksi useat artiklat jättävät tavallaan mahdollisuuden kansalliselle sääntelylle, mutta monet näistä edellyttäisivät yksityiskohtaisempaa lakia, joten todennäköisesti niiden sääntely jää täysin asetuksen mukaiseksi. Esimerkkejä tällaisista artikloista ovat muun muassa henkilötietojen käsittelyä koskevat periaatteet sekä kaikki rekisteröityjen oikeuksia koskevat kohdat. Vaikka asetuksen 23 artikla antaisi mahdollisuuden esimerkiksi rekisteröidyn oikeuksien rajoittamiselle, ei sellaisen täytäntöönpanemista voitaisi kovin helposti perustella yhteiskunnallisesti välttämättömäksi.

Mahdollisen kansallisen liikkumavaran lisäksi useat GDPR:n artiklat jopa edellyttävät asian huomioimista jäsenvaltion omassa lainsäädännössä. Tällaisia huomioinnin ja velvollisuuden jaottelun alle meneviä tietosuojan osa-alueita ovat esimerkiksi useat tietosuojavastaavaan sekä valvontaviranomaiseen liittyvät asiat (OM: TATTI 2017, 56, 58). Notifiointivelvollisuuden alaisten artikloiden kohdalla jäsenvaltiolla on velvollisuus ilmoittaa Euroopan komissiolle, kuinka kyseistä määräystä, eli tässä tapauksessa tietosuoja-

asetusta, on noudatettu. Käytännössä tämä tarkoittaa sitä, että jokaisen jäsenvaltion tulee itse määrittää oma valvontaviranomainen sekä tämän kelpoisuuteen ja perustamiseen liittyvät seikat. Tästä huolimatta valvontaviranomaisen toimivalta ei kuitenkaan jätä kansallista liikkumavaraa (OM: TATTI 2017, 60). Suomessa valvontaviranomaisen roolissa toimii jatkossa tietosuojavaltuutettu (HE 9/2018, 3.5).

Kansalliseen liikkumavaraan liittyvät periaatteet voivat tuntua monimutkaisilta, mutta niiden soveltaminen ei kosketa yritysten jokapäiväistä toimintaa. Tästä huolimatta yritysten kannattaa seurata lainsäädännön kehitystä, etenkin silloin, kun tietosuoja-asioissa tulee vastaan epäselvyyksiä. Suomen lainsäädäntöön asetettava tietosuojalaki tulee toimimaan ikään kuin Suomeen räätälöitynä versiona EU:n asetuksesta, joten yritysten on helppo tarkistaa sen sisällöstä tietosuojasäädöksiä. Kansallisella lainsäädännöllä tuskin tullaan koskaan poikkeamaan GDPR:n asettamista velvoitteista huomattavasti, joten asetusta noudattamalla toimii lainsäädännöllisesti aina oikein.

4 TJB-YHTIÖT OY

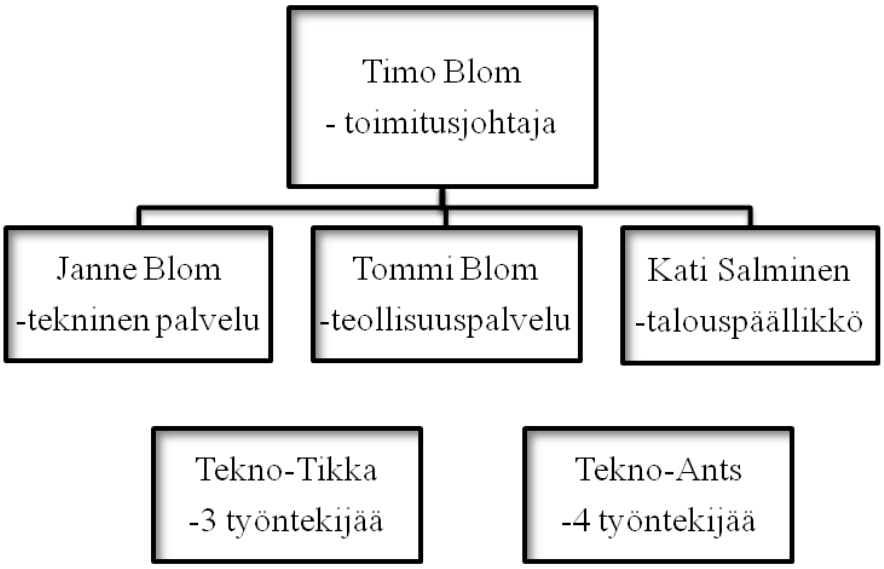
TJB-Yhtiöt Oy on vuonna 1996 perustettu perheyhtiö, joka toimii omistamallaan liikekiinteistöllä Tampereella. Yhtiön tehtävä on hallinnoida omistamiaan Tekno-Yhtiöitä. (Tekno-Tikka) TJB-Yhtiöt Oy:llä on 100 % omistusosuus kahdesta tytäryhtiöstään Tekno-Tikasta sekä Tekno-Antsista. (Salminen 2017)

Tytäryhtiö Tekno-Tikka on sähköautomaation alalla toimiva osto-myyntiliike, joka panostaa toiminnassaan vahvaan tekniseen osaamiseen sekä henkilökohtaiseen asiakaspalveluun. Tekno-Tikka kehittää muun muassa ainutlaatuisia ratkaisuja jätteenkäsittelyn optimointia varten. (Salminen 2017) Toinen tytäryhtiö Tekno-Ants taas on start-up yhtiö, joka valmistaa apurobotteja esimerkiksi teollisuuden ja maatalouden materiaalikuljetusten avuksi. (Tekno-Ants) TJB-Yhtiöt Oy:n talouspäällikkö Kati Salmisen (2017) mukaan Tekno-Antsin toiminta on vasta alkutekijöissään, mutta yhtiön potentiaali on valtava.

TJB-Yhtiöt toimii näin ollen konsernissa emoyhtiönä tytäryhtiöille Tekno-Tikalle sekä Tekno-Antsille. Molemmat konserniyhtiöt saavat TJB-Yhtiöiltä hallintopalveluna henkilöstö- ja taloushallinnon. (Salminen 2017) Toisin sanoen toimeksiantajayritys hoitaa näiden kahden yhtiön henkilöstö- sekä talousasiat.

4.1 Organisaatio

TJB-Yhtiöt Oy:n alla työskentelee yhteensä 11 henkilöä. Nämä työntekijät ovat jakautuneet yhtiöiden kesken siten, että kolme työskentelee Tekno-Tikalla, neljä Tekno-Antsilla ja neljä varsinaisella emoyhtiöllä. (Salminen 2017) Toimeksiantajayhtiön keskeisimmät henkilöt on esitelty organisaatiokaavion avulla.



KUVIO 2. Organisaatiorakenne

Kaikkien yhtiöiden toimitusjohtaja Timo Blom on TJB-Yhtiöt Oy:n pääosakas. Hän osallistuu myös vahvasti yhtiöiden myyntitoimintaan. Janne Blom toimii toimitusjohtajan sijaisena sekä prokuristina, eli hänellä on valtuutus toimia yhtiön puolesta (Prokuralaki 1979, 2 §). Janne Blomin vastuulla ovat myös tuotekehitys, tekniset ratkaisut sekä atk-kehitys. Tommi Blom on mukana sekä Tekno-Tikan että Tekno-Antsin toiminnassa aina valmistuksesta myyntiin asti. Edellä mainitut henkilöt kuuluvat yhtiön hallitukseen yhdessä Timo Blomin kahden tyttären kanssa. (Salminen 2017)

Yhtiön hallinnollisia juoksevia asioita hoitaa talouspäällikkö Kati Salminen. Hänen vastuullaan on henkilöstö- ja taloushallinnon hoitaminen, joten hänen roolinsa tietosuoja-asioissa on olennainen. (Salminen 2017)

4.2 Henkilötietojen käsittely

TJB-Yhtiöiden osalta henkilötietojen käsittely koskee pääsääntöisesti henkilökunnan palkka- sekä terveystietoja. Näitä tietoja yhtiössä käsittelee tällä hetkellä muutama ihminen, ja tietoja säilytetään sekä sähköisessä että paperisessa muodossa. (Salminen 2017) Tietosuojauudistukseen valmistautumisen olennainen osa on tarkastella tämänhetkisiä

henkilötietojen käsittelyprosesseja, jotta voidaan varmistua siitä, että käsittely on ensin myös nykyisen kansallisen lainsäädännön mukaista (Tietosuojavaltuutetun toimisto 2018).

4.2.1 Palkkatiedot

Yhtiöiden työntekijöiden palkkatietoja löytyy palkka-aineistosta sekä henkilöstöluettelosta, joka on Excel-ohjelmassa muodostettu ja ylläpidetty taulukko. Tähän luetteloon on pääsy talouspäällikkö Kati Salmisen lisäksi toimitusjohtaja Timo Blomilla. Itse palkka-aineiston käsittely ja säilytys kuuluu vain Salmisen vastuulle. Tätä aineistoa löytyy Salmisen sähköpostista, henkilökohtaiselta verkkoasemalta sekä paperimuodossa kansioista. Tietokoneiden pääkäyttäjäoikeudet ovat Janne Blomilla, joka näin ollen pystyy tarkastelemaan sekä sähköpostia että verkkolevyn tiedostoja. Vanhempaa palkka-aineistoa säilytetään arkistokaapeissa, joiden avain on vain talouspäällikön käytössä. (Salminen 2017)

Yhtiön palkanlaskenta on ulkoistettu Accountor Tampere Oy:lle, joka välittää palkkatietoja talouspäällikölle sähköpostitse. Tällä hetkellä sähköpostiyhteyttä ei ole suojattu. (Salminen 2017)

Henkilötietolain (523/1999 32 §) mukaan rekisterinpitäjän tulee tehdä tarvittavat toimenpiteet, jotta henkilötiedot eivät joudu asiattomien käsiin, eikä tietoja käsitellä laittomasti. Tällä hetkellä TJB-Yhtiöt Oy:n palkkatiedot ovatkin rajattu lainmukaisesti vain niiden käsittelyn kannalta olennaisten ihmisten saataville.

4.2.2 Terveystiedot

Työntekijöiden sairaslomatodistukset kulkevat talouspäällikön kautta palkanlaskentaan sähköpostilla. Alkuperäisiä todistuksia säilytetään tällä hetkellä kansioissa muun palkka-aineiston kanssa. (Salminen 2018)

Työelämän tietosuojalaki (759/2004) säätää terveydentilaa koskevien tietojen mahdollisesta käsittelijästä sekä säilytystavasta. Lain viidennen pykälän mukaan tietoja saa käsitellä vain työsuhteen päätöksien kannalta olennainen henkilö, ja terveyttä koskevia tietoja

tulee säilyttää erillään muista kerätyistä henkilötiedoista. Tämän perusteella yhtiön kannattaisi tarkistaa, että sairaslomatodistukset säilytetään eri kansioissa ja mahdollisesti myös eri paikassa, kuin palkka-aineisto. Näin terveystietojen säilytys olisi kansallisen lainsäädännön tasolla.

5 ASETUKSEN VAIKUTUKSET TJB-YHTIÖT OY:HYN

GDPR:n tulosta on varoitettu yrityksiä jo pitkään. On ymmärrettävää, että jokainen yritys kokee pelotteet uusista hallinnollisista sakoista uhkana ja haluaa varmistaa, ettei rangaistus osu omalle kohdalle. Yrityksissä, joissa tietosuoja-asioita ei ole hoidettu lainkaan, on tarve muuttaa toimintaa asetuksen mukaiseksi, mutta mikäli yritys on aiemmin toiminut jo voimassaolevan lainsäädännön mukaisesti, ovat muutostarpeet suurimmalle osalle melko pieniä. TJB-Yhtiöt Oy, kuten moni muukin pk-yritys, teki hyvän ratkaisun ulkoistaessaan asetuksen käsittelyn, sillä resurssien vuoksi asian selvittäminen olisi voinut jäädä hyvin pintapuoleiseksi. Tämä osio tiivistää asetuksen merkitystä toimeksiantajayhtiölle ja sisältää konkreettisia suosituksia tehtävistä toimenpiteistä.

Asian lähestymisen voi aloittaa TJB-Yhtiöiden roolin määrittelystä. Yhtiö toimii tarkasteltavassa tilanteessa rekisterinpitäjänä ja yhtiön työntekijät rekisteröityinä. Näin ollen tässä työssä luetellut rekisterinpitäjän velvollisuudet ja rekisteröidyn oikeudet koskevat yhtiön toimintaa. Yhtiön koon ja käsiteltävien henkilötietojen vuoksi kaikki asetuksessa mainitut seikat eivät tule sovellettavaksi, joten niiden käsittely jätetään tässä yhteydessä vähälle.

TJB-Yhtiöt Oy:n henkilötietojen käsittelyn lainmukaisuudelle on hyvä etsiä peruste asetuksen 6 artiklasta. Työnantajan aseman vuoksi voidaan olettaa, että henkilötietojen käsittely on tarpeellista lakisääteisten velvollisuuksien kuten palkan- ja veronmaksun noudattamisen kannalta. Lainmukaisuuden perusteeksi luetaan tässä tapauksessa myös 6 artiklan f) -kohdassa mainittu oikeutettu etu. Yhtiössä rekisterinpitäjän ja rekisteröidyn välillä on suhde, jossa kummankin osapuolten etujen saavuttamiseksi henkilötietojen käsittely on välttämätöntä.

5.1 Suositukset toimenpiteistä

Tulevia toimenpiteitä suunniteltaessa tulee muistaa suhteuttaa toimenpiteet olemassa olevaan riskiin. Tärkeää on olla perillä nykytilanteesta, jotta pystytään kartoittamaan osa-alueet, joissa on mahdollisesti parantamisen varaa. Vaikka tässä työssä on tehty melko

kattava kartoitus yhtiön henkilötietojen käsittelystä, kannattaa silti yhtiössä vielä varmistaa, ettei henkilötietoja enää löydy paikoista, missä niitä ei odotettu olevan.

Nämä suositeltavat toimenpiteet ovat suoraan johdannaisia asetuksen asettamista periaatteista. Yhtiön kannattaa kuitenkin aktiivisesti ylläpitää ja päivittää tietosuojakäytänteitä, etenkin silloin, jos/kun tilanteet muuttuvat. Tässäkin yhtiön kannattaa aina pitää mielessä suhde riskeihin sekä resurssien järkevä käyttö. Yhtiön kannalta tämä tarkoittaa käytännössä sitä, että mitä pienemmällä vaivalla ja ajalla tietosuoja-asioiden muuttamisesta ja hoitamisesta voidaan selvitä, sen parempi.

5.1.1 Tietosuojan keskittäminen

TJB-Yhtiöiden kannalta olisi hyvä, että tietosuoja-asioiden hoitamisesta ottaisi joku vastuun. Tällä hetkellä tietosuojaa ei mitenkään laiminlyödä, mutta tulevaisuuden kannalta kannattaisi yhtiöstä löytyä joku henkilö, joka esimerkiksi osaa vastata tietosuojaa koskeviin kysymyksiin ja tietää, mitä kaikkea lainsäädäntö edellyttää. Tämä ikään kuin pienemmän mittakaavan tietosuojavastaava voisi hoitaa ilmoitukset mahdollisista tietoturvaloukkauksista ja varmistaa, että henkilötietojen käsittely pysyy aina hyvällä tasolla.

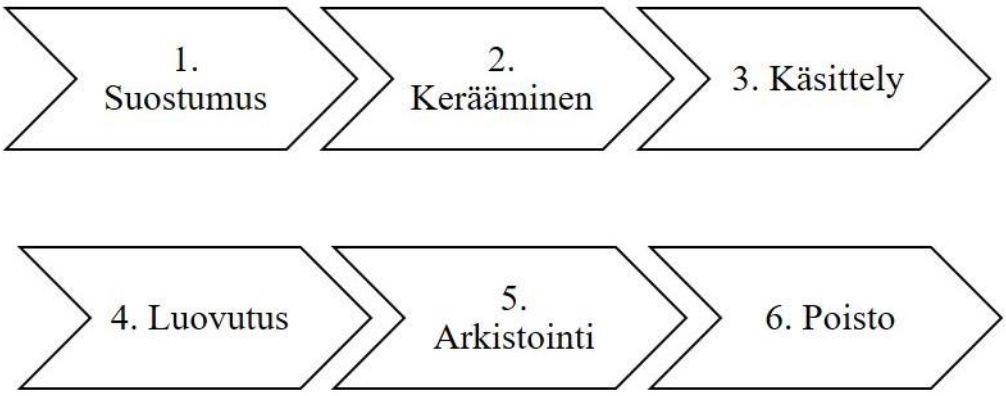
Resurssien vuoksi on selvää, ettei tietosuoja-asioiden selvittelylle voida uhrata yhdeltä ihmiseltä paljoa aikaa, mutta käytännössä tämä vastuu tulee eteen lähinnä ongelmatilanteissa tai muuttuvissa olosuhteissa. Tähän rooliin sopiva henkilö olisi esimerkiksi talouspäällikkö, sillä hänen työnkuvaansa sisältyy jo valmiiksi henkilötietojen käsittelyä ja hänen vastuullaan suurin osa tietojen säilyttämisestä on jo nyt. Näin ollen eniten henkilötietoja käsittelevällä olisi myös eniten tietoa tietosuojalainsäädännöstä, ja todennäköisyys asetuksen vastaisille rikkeille olisi pieni.

5.1.2 Henkilötietojen säilytys ja siirtäminen

Asetus ei varsinaisesti ota kantaa sähköpostin kautta liikkuviin tietoihin, mutta koko asetuksen ydintarkoituksiahan on turvata henkilötiedot digitalisoituvassa ympäristössä. Viestintäviraston (2017) mukaan luottamuksellista tietoa sisältävät sähköpostit kannattaa aina salata. Toimeksiantajayhtiö oli jo suunnitellut suojatun sähköpostiyhteyden hankki-

mista ja tämä suunnitelma kannattaa ehdottomasti toteuttaa. Yhtiön palkanlaskentaan lähettämät palkkatiedot sisältävät työntekijöiden henkilötunnuksia ja muuta tietoa, joka vuotaessaan voisi aiheuttaa rekisteröidyille huomattavia oikeuksien menetyksiä. Näitä tietoja koskevia tietoturvaloukkauksia voidaankin pitää yhtiön kannalta suurimpina riskitekijöinä. Suojatun sähköpostin lisäksi on hyvä varmistaa, että palomuurit ja muut tekniset suojauskeinot ovat aina toiminnassa.

Kuten aiemmin mainittiin, paperiset tiedostot työntekijöiden terveystiedoista kannattaa siirtää eri paikkaan, kuin missä palkka-aineisto on. Tätä seikkaa lukuun ottamatta, tietojen säilytys on asetuksen tasolla, sillä arkistokaapit ovat lukitut, eikä niihin pääse käsiksi kukaan, joka ei ole siihen oikeutettu. Kaikkien näiden tietojen säilytyksessä on kuitenkin hyvä pitää mielessä tiedon elinkaari eli henkilötiedon vaiheet yhtiön toiminnassa.



KUVIO 3: Tiedon elinkaari. (Perustuu VAHTI-raportin (VM 2016, 24) malliin)

Ylläolevassa kaaviossa on rekisterinpitäjän kannalta olennaisimmat vaiheet henkilötiedon käsittelylle. Yhtiön kannalta työnantajana on tärkeää huolehtia vaiheiden lainmukaisesta toteutumisesta ja muistaa, että myös tietojen hävittäminen kuuluu tietojenkäsittelyprosessiin. Tämä tarkoittaa käytännössä sitä, että aina kun uutta tietoa kerätään, tulee tietää kuinka kauan sitä saa/täytyy säilyttää, sillä tämä tieto on tarpeen vaatiessa esitettävä myös rekisteröidylle. On hyvä myös huolehtia siitä, ettei tarpeetonta tietoa jää säilymään sähköpostiin tai arkistoihin esimerkiksi entisistä työntekijöistä.

Yksi vaihtoehto tiedon turvalliseen säilytykseen ja lähettämiseen olisi pseudonymisoida henkilötietoja eli muokata tietoja sellaiseen muotoon, että työntekijät eivät olisi enää tunnistettavissa asiakirjoista ilman lisätietoja. Tämän voisi toteuttaa esimerkiksi tiedoille annettavilla numerotunnisteilla, joiden selitys löytyisi erillisestä paikasta niin, ettei näitä kahta tietoa pystyisi yhdistämään. TJB-Yhtiöt Oy:n osalta pseudonymisointi ei tämänhetkisessä tilanteessa ole tarpeellista, mutta siitä huolimatta tällaisesta suojauskeinosta on hyvä olla tietoinen.

5.1.3 Ulkoiset henkilötietojen käsittelijät

Palkanlaskenta toimii yhtiölle henkilötietojen käsittelijänä, jolle yhtiö antaa henkilötietoja, jotta palkanlaskenta voi käyttää niitä toimiessaan yhtiön hyväksi. Sinänsä tämä ei aseta henkilötietojen suojalle erityistä riskiä, muuten kuin sähköpostin osalta, mutta on paikallaan tarkastella palkanlaskennan kanssa tehtyä sopimusta. Nykyinen asetus vaatii tällaiselta tietojenkäsittelysopimukselta hieman entistä lainsäädäntöä enemmän, joten on sekä yhtiön että palkanlaskennan edun mukaista, että sopimus päivitetään asetuksen ohjeiden mukaiseksi. Näin kummatkin osapuolet pysyvät tietoisena sovituista asioista ja siitä, mitä on sitouduttu noudattamaan (Hanninen ym. 2017, 83).

Tietojenkäsittelysopimukseen kannattaa sopia kaikki tiedot käsittelytoimista, kuten käsittelyn kohteesta ja tarkoituksesta sekä kestosta. Myös yhtiön ja palkanlaskennan velvollisuudet ja oikeudet on hyvä löytyä kirjallisesta sopimuksesta. (Hanninen ym. 2017, 83) Yhtiöllä on varmasti olemassa jo kirjallinen sopimus palkanlaskennan kanssa, mutta kannattaa selvittää onko myös heidän puoleltaan tarpeen tehdä esimerkiksi tarkennuksia uuden asetuksen johdosta. Asian eteenpäin viemiseksi yhtiön kannattaa olla yhteydessä palkanlaskentaan, mikäli he eivät vielä ole asian tiimoilta ottaneet yhtiöön itse yhteyttä.

5.1.4 Dokumentaatio

Osoitusvelvollisuus oli yksi suurimmista muutoksista, joita GDPR toi tietosuojalainsäädäntöön, sillä yhtiö tarvitsee nyt konkreettisen kirjallisen osoituksen siitä, miten henkilötietojen käsittely hoituu yhtiön jokapäiväisessä toiminnassa. Yhtenä osana tätä työtä TJB-Yhtiöt Oy:lle luotiin valmis seloste käsittelytoimista (Liite 1.), josta ilmenee yhtiön tietosuojapolitiikka ja sitä hoitavat henkilöt. Tämän asiakirjan yhtiö voi tarvittaessa esittää

asiaa tiedustelevalle, ja sitä voidaan pitää yhtiössä myös ikään kuin ohjeena siitä, miten tietosuoja-asioiden kanssa toimitaan.

Seloste on pyritty toteuttamaan niin, että se sisältää kaiken olennaisen tiedon TJB-Yhtiöt Oy:n toiminnasta ja riittää suurilta osin toteuttamaan yhtiön osoitusvelvollisuutta. Tulee muistaa, että yhtiön käsittelemien henkilötietojen alue ei ole kovin laaja, joten dokumentaation ei ole tarvetta sisältää esimerkiksi laajoja riskiarviointeja tai prosessikertomuksia. Tästä huolimatta dokumentaatio on kirjoitettu niin, että siihen jää tilaa tulevaisuuden muokkauksille. Mahdollisia muokkaustarpeita voi esiintyä esimerkiksi käytänteiden muuttuessa tai mikäli yhtiön tietoturva kokee jonkin loukkauksen. Tällaisissa tilanteissa on toki hyvä arvioida dokumentaation lisäksi myös tilanteen vaikutusta tietoihin kohdistuviin riskeihin. Yhtiön kannattaa selostetta muokatessa tarkistaa tietosuoja-asetuksen 30 artiklasta, että kaikki tarvittavat tiedot löytyvät edelleen kirjallisesta dokumentaatiosta.

Seloste käsittelytoimista on liitetty tähän työhön ja lisäksi se on lähetetty yhtiön talouspäällikölle sähköpostilla erillisenä tiedostona. Tämä tekee sen erillisestä käsittelystä ja muokkauksesta yhtiölle helpompaa. Dokumentaation rakentamisessa on hyödynnetty Tietosuojavaltuutetun toimiston asettamaa ohjeistusta (2018) sekä asetuksen 30 artiklaa.

5.2 Henkilöstön tietoisuus

Tietosuoja-asioiden olisi hyvä olla jossain määrin koko henkilöstön tiedossa, vaikka vain kourallinen yhtiön henkilökunnasta tosiasiassa käsittelee henkilötietoja. Todennäköisesti työntekijät eivät ole täysin tietoisia asemistaan rekisteröityinä tai tietosuojalainsäädännössä heille turvatuista oikeuksista. Toki TJB-Yhtiöt Oy käsittelee henkilötietoja sellaisin työsuhteeseen liittyvin perustein, ettei kaikkia rekisteröidyn oikeuksia pysty täysin soveltamaan. Tietosuoja-asiat kuitenkin tulevat koko ajan ajankohtaisemmiksi ja digitalisoituminen asettaa omat riskinsä työntekijöiden henkilötiedoille. Vaikka tietoturvan varmistaminen jääkin johdon ja henkilötietoja ensisijaisesti käsittelevien henkilöiden vastuulle, olisi yhtiön kannalta erittäin hyvä, mikäli koko henkilökunta ymmärtäisi tietosuojan merkityksen myös pienessä yrityksessä. Näin yhtiö pystyisi kokonaisuutena luottamaan siihen, että millään osa-alueella ei tahallisesti tai tahattomasti loukata tietosuojaa.

Hyvä keino tietosuojaymmärryksen levittämiseen olisi esimerkiksi kehottaa henkilöstöä lukemaan tämä opinnäytetyö, joka melko tiiviisti selostaa olennaiset osat pian sovellettavaksi tulevasta EU:n tietosuoja-asetuksesta. Henkilöstölle olisi myös hyvä tehdä selväksi, kuka yhtiössä osaa vastata tietosuojaa koskeviin kysymyksiin. Tämän työn lähteistä löytyy myös paljon lisää luotettavaa materiaalia tietosuoja-asioista, mikäli henkilöstö haluaa perehtyä asiaan vielä tarkemmin.

5.3 Yhtiön tietosuojatulevaisuus

TJB-Yhtiöt Oy:llä on tiiviin henkilöstönsä vuoksi kaikki valttikortit viedä tietoturvallisuus todella hyvälle tasolle. Yhtiön ei kannata nähdä tietosuojaa asiana, joka estäisi tai hidastaisi toimintaa, vaan enemmänkin luottamuksenrakentajana henkilöstön ja johdon välillä sekä kehityksen mahdollistajana (Andreasson ym. 2016, 19-21). Pienessä yrityksessä voi olla haastavaa välillä nähdä tietosuojaa näin mittavana tekijänä, mutta mitä suuremman roolin tietosuoja saa yhteiskunnassa, sitä arvostetummaksi koetaan yrityksiä, joissa tietosuojaan panostetaan.

Tällä työllä on nyt luotu ikään kuin kehykset yhtiön tulevaisuuden tietosuojatoiminnoille, mutta lopullinen vastuu huolellisuuden toteuttamisesta jää yhtiön johdolle. Tärkeänä seikkana voidaan mainita se, että yhtiön kannattaa varautua kaikenlaisiin muutoksiin tietosuojasäädäntöä koskien. Tällä hetkellä monet käytännöt ovat vapaaehtoisia tai eivät edellytä jatkuvia toimenpiteitä, mutta aina on hyvä seurata tilanteiden kehittymistä, jotta mahdolliset uudistukset tai tarkastukset eivät pääse yllättämään. Lähtökohtaisesti voidaan todeta, että yhtiön ei tarvitse tulevaisuudessa alkaa pelkäämään miljoonien sakkorangaistusta, vaan sen sijaan tietosuoja kannattaa ottaa avoimin mielin yhdeksi osaksi yhtiön perusperiaatteita.

6 POHDINTA

EU:n yleisen tietosuoja-asetuksen saapumista on peloteltu yrityksille jo jonkin aikaa, vaikka se ei ydinsisällöltään kovin suuresti poikkea nykyisestä lainsäädännöstä. Ensisilmäyksellä asetuksen sääntely tuntuu pk-yrityksen kannalta hyvinkin raskaalta, sillä monissa yrityksissä tietosuoja-asioiden on annettu ikään kuin rullata omalla painollaan. Olennaiseksi asetukseen perehtymisessä osoittautuikin sääntelyn tulkitseminen niin, että asetuksesta löytyy tärkeät kohdat pienelle yritykselle ja toisaalta myös ne kohdat, jotka eivät koske TJB-Yhtiöt Oy:n kaltaisten yritysten toimintaa.

Rekisterinpitäjän vastuuta ei voi kuitenkaan kieltää, vaikka yrityksen toiminta olisi hyvinkin pienimuotoista. Näin ollen voidaan tulkita myös hyvänä asiana, että yrityksille on maalattu suuria uhkakuvia asetuksen rikkomisen sakoista. Riskien uhalla yritykset alkavat selvittää omia tietosuojakäytänteitä ja tietoisuus asioista lisääntyy. Kukaan luonnollinen henkilö ei varmasti halua omien henkilökohtaisten tietojensa joutuvan tietoturvaloukkauksen kohteeksi, joten mitä suurempi osa yrityksistä alkaa avoimesti kunnostamaan tietosuojapolitiikkaansa, sitä parempi. Asetuksen sääntelystä voidaan päätellä, että yrityksen kannalta on järkevämpää ylimitoittaa varautumisensa tietoturvaloukkauksiin ja mahdollisiin viranomaistarkastuksiin, kuin luottaa siihen, että mitään ei todennäköisesti tule tapahtumaan.

Tämän opinnäytetyön tavoitteena oli selvittää asetusta ja sen vaikutuksia TJB-Yhtiöt Oy:n tietosuojatoimintaan. Tämä tavoite toteutui lähinnä lainopillisen tutkimuksen kautta, sortumatta silti liialliseen lakitekstin ja säädöshistorian analyysiin. Tutkimuksen merkittävimpänä tuloksena selvisi, että asetus tuo jonkin verran kiristyneempää sääntelyä rekisterinpitäjän velvollisuuksiin sekä niiden rikkomisesta aiheutuviin sanktioihin. Suoranaisesti asetuksesta ei löytynyt yhtiötä koskevia suuria velvoitteita, vaan antamani suositukset koskivat lähinnä toiminnan yhdenmukaistusta ja tietoturvaloukkauksiin varautumista. Osa-alueista suurimmin huomiota kaipasi tietojen säilyttäminen sekä manuaalisessa että ATK-muodossa. Yhtiön toiminnan muuttaminen asetuksen mukaiseksi ei onneksi vaadi yhtiöltä kovin mittavia toimenpiteitä, sillä aikaa näiden toimenpiteiden toteuttamiselle ei ennen asetuksen tuloa olisi välttämättä jäänyt. Kuten työn yhtenä merkit-

tävimmistä tarkoituksista oli, yhtiö sai heti tämän opinnäytetyön myötä käyttöönsä selosteen käsittelytoimista, jota yhtiö voi sellaisenaan hyödyntää tietosuojatoiminnassa. Työn tavoitteet toteutuivat näin ollen suunnitellun mukaisesti.

Opinnäytetyöhön oli alun perin tarkoitus sisällyttää kysely yhtiön johdolle tai työntekijöille, mutta tämä jäi tietoisen valinnan perusteella työstä pois. Vaikka kysely olisi tuonut lisää sisältöä ja empiiristä tutkimusta työhön, ei sen hyöty yhtiön kannalta olisi ollut kovin suuri. Tämä kysely osoittautui ainoaksi osaksi, joka löytyi alkuperäisestä suunnitelmasta, mutta ei päätynyt lopulliseen työhön. Alkuperäinen suunnitelma toteutui myös aikataulullisesti lähes kokonaan, ja työ pysyi aikomuksien mukaisesti tiiviinä kokonaisuutena, jossa aiheen käsittelyä ei päästetty leviämään yli tarpeellisten rajojen.

Työ toteutui hyvin lyhyessä ajassa, joten kirjoittamisvaiheen yhteydenotot toimeksiantajayhtiöön jäivät hieman vähälle. Haastavaksi osoittautui myös lähdekirjallisuuden etsiminen, sillä aiheen ajankohtaisuuden vuoksi monet teokset olivat hyvin haluttuja tai ilmestyivät vasta myöhemmin. Tästä syystä työssä hyödynnetty aineisto jäi hieman suppeammaksi, kuin mitä toivoin. Useat tietosuojaa koskevat verkkosivustot elävät myös uuden vaiheen edeltävää aikaa, joten niiden sisältämä tieto tarkentuu ja muokkautuu lähes päivittäin. Ajankohtaisuus toi toki haastavuuden lisäksi aiheeseen mielenkiintoa, sillä EU:n yleinen tietosuoja-asetus tuntuu olevan puhutuin aihe yritysmaailmassa tällä hetkellä. Työssä kiteytyi olennaisesti asetuksen sisältö tavallisen pk-yrityksen kannalta ja haasteista huolimatta työ palvelee toimeksiantajayhtiön toiveita hyvin.

TJB-Yhtiöt Oy:ssä on ryhdytty toteuttamaan tämän opinnäytetyön sisältämiä ehdotuksia välittömästi. Tietoarkistojen läpikäyminen on aloitettu hyvissä ajoin, jotta tarpeeton tieto saadaan hävitettyä ja tarpeellinen tieto järjestettyä turvallisella tavalla. Muutoksiin varaudutaan koko yhtiön johdon voimin ja talouspäällikkö pyrkii tiedottamaan henkilöstölle tulevista tietosuojatoimenpiteistä. Toimeksiantaja on tyytyväinen opinnäytetyön lopputulokseen ja valmis heti hyödyntämään tutkimuksen tuloksia sekä dokumentaatiota konkreettisesti toiminnassaan.

Tietosuojalainsäädäntö tulee mukautumaan yhteiskunnan tarpeisiin myös asetuksen jälkeen, joten jatkotutkimusaiheita henkilötietojen käsittelystä löytyy useita. Tässä työssä käsiteltävän GDPR:n jatkotutkimuksena voisi esimerkiksi vertailla kahden pk-yrityksen

henkilötietojen käsittelyä ja asetuksen noudattamista. Yksi mielenkiintoisimmista tavoista tutkia tietosuojaa eteenpäin olisi perehtyä uudistuvaan EU:n sähköisen viestinnän tietosuojadirektiiviin, jonka vaikutuksia voisi tutkia esimerkiksi suuremman yrityksen verkkomainonnan tai viestiliikenteen kannalta.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. 3. painos. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma Oy.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma Oy.

Euroopan komissio. Mikä on rekisterinpitäjä tai tietojen käsittelijä? Luettu 23.4.2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi

Euroopan parlamentin ja neuvoston asetus 2016/679/EU, annettu 27. päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (EU:n yleinen tietosuoja-asetus).

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi 9/2018

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Helsingin Kauppakamari Oy.

Henkilötietolaki 22.4.1999/523

Honkinen, T., Innanen, A., Lindgren, J., Pello, J., Rantanen, J., Siltala, K. & Tuomala, S. 2016. Startup-juridiikan käsikirja. Alma Talent Oy.

Elo, E. Kauppalehti. 16.8.2017. Useiden pk-yritysten tietoturvassa puutteita. Luettu 27.3.2018 https://www.kauppalehti.fi/uutiset/useiden-pk-yritysten-tietoturvassa-puutteita/8X6ZiGjR

Laki yksityisyyden suojasta työelämässä 759/2004

Nyyssölä, M. 2017. Yksityisyyden suoja työsuhteessa. Alma Talent Oy.

Oikeusministeriö 1.3.2018. Tietosuojalaki täydentäisi EU:n tietosuoja-asetusta. Luettu 27.3.2018 http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta

Oikeusministeriö 35/2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Mietintöjä ja lausuntoja. Luettavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf?sequence=1&isAllowed=y

Oikeusministeriö 4/2017. Miten valmistautua EU:n tietosuoja-asetukseen? Tietosuojavaltuutetun toimisto. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

OpiTietosuojaa 2017. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Luettu 26.3.2018. Kuvio 1 otettu verkkosivulta 26.3.2018 https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus

Pitkänen, O., Tiilikka, P. & Warma, E. 2013. Henkilötietojen suoja. Alma Talent Oy.

Prokuralaki 2.2.1979/130

Salminen, K. talouspäällikkö. 2017. TJB-taustatietoa. Sähköpostiviesti. kati.salminen@teknotikka.fi. Luettu 21.9.2017.

Salminen, K. talouspäällikkö. 2018. Re: TJB-taustatietoa. Sähköpostiviesti. kati.salminen@teknotikka.fi Luettu 25.1.2018.

Suomen perustuslaki 11.6.1999/731

Tekno-Ants. Logistiikka. Luettu 14.3.2018 http://www.teknoants.fi/logistiikka

Tekno-Tikka. Yritys. TJB-Yhtiöt Oy. Luettu 14.3.2018. http://teknotikka.fi/yritys/

Tietosuojavaltuutetun toimisto. 2018. EU:n tietosuojauudistus. Luettu 26.3.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tietosuojavaltuutetun toimisto. 23.3.2018.Seloste käsittelytoimista. Luettu 3.4.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/seloste-kasittelytoimista.html#mitatietojaselosteessataytyyolla

Valtiovarainministeriö 1/2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Vanto, J. 2011. Henkilötietolaki käytännössä. Alma Talent Oy.

Viestintävirasto. 3.10.2017. Sähköpostin tietoturva. Luettu 30.3.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/sahkoposti.html

LIITTEET

Liite 1. Dokumentaatio

SELOSTE KÄSITTELYTOIMISTA

Tämä asiakirja osoittaa TJB-Yhtiöt Oy:n käsittelevän henkilötietoja EU:n yleisen tietosuoja-asetuksen mukaisesti. Selostetta päivitetään tarvittaessa.

Laadittu: 1.4.2018

Päivitetty:

1. Rekisterinpitäjä

- TJB-Yhtiöt Oy
- Y-tunnus: 1070677-9
- Osoite: Lumpeenkatu 1, 33900 Tampere
- Puhelin: 020 7464880

2. Yhteyshenkilö

- Kati Salminen, talouspäällikkö
- kati.salminen@teknotikka.fi

3. Henkilötietojen käsittelytarkoitus

Käsittelemme toiminnassamme työsuhteen kannalta olennaisia henkilötietoja työntekijöistämme. Henkilötietojen käsittely kohdistuu vain tarpeelliseen tietoon, eikä tietoja käytetä muuhun, kuin työsuhteen oikeuksien ja velvollisuuksien toteuttamiseen. Käsittelemme ja säilytämme tietoja vain tarpeellisen ajan, jonka jälkeen hävitämme ne asianmukaisesti.

Työntekijöidemme henkilötietoja ei luovuteta säännönmukaisesti muille tahoille, eikä niitä siirretä EU:n ulkopuolelle.

4. Tietosisältö

- Työntekijöiden yksilölliset tiedot kuten nimi, osoite ja henkilötunnus
- Palkkatiedot
- Terveydentilatiedot

Rekisterimme sisältää palkanmaksun ja työsuhteen ylläpidon kannalta olennaisia tietoja. Terveydentilatietoja käsittelemme vain palkanlaskennan vuoksi sairaslomatodistusten muodossa. Keräämme ensisijaisesti kaiken tiedon työntekijöiltä itseltään.

5. Henkilötietojen ulkoinen käsittelijä

Palkanlaskentamme on ulkoistettu Accountor Tampere Oy:lle, jolle toimitamme säilyttämiämme henkilötietoja sähköpostin välityksellä. Palkanlaskennan kanssa on tehty tietojenkäsittelysopimus, josta ilmenee molempien osapuolten oikeudet ja velvollisuudet. Pidämme huolen siitä, että sopimus pysyy ajan tasalla.

6. Suojaustoimenpiteet

Lähetämme henkilötietoja sisältävät sähköpostit suojattujen yhteyksien kautta. Myös verkkoasemalta löytyvät henkilötietoja sisältävät tiedostot ovat suojattu henkilökohtaisiksi, eikä niitä pysty tarkastelemaan muut, kuin niihin oikeutetut työntekijät. Sähköiset tietomme ovat lisäksi suojattu salasanojen ja palomuurien avulla.

Manuaalista aineistoa henkilöstön palkka- ja sairaslomatiedoista säilytetään lukituissa arkistokaapeissa, joiden avain on vain talouspäällikön hallinnassa. Asiattomilla ei ole pääsyä fyysiseen henkilötietoaineistoon. Arkaluonteisempia terveystietoja säilytetään lisäksi erillään muusta aineistosta.

Huolehdimme aktiivisesti, että hallussamme olevia henkilötietoja käsitellään luottamuksellisesti sekä vain niiden toimesta, joiden työnkuvan kannalta käsittely on olennaista.

7. Rekisteröityjen oikeudet

Työntekijöillämme on tiedossa yhteyshenkilö, joka osaa avustaa tietosuojaa koskevissa asioissa. Jokaisella työntekijällämme on oikeus halutessaan saada tietää, mitä henkilötietoja hänestä on yhtiömme hallussa. Tietosuojatoimillamme pyrimme turvaamaan työntekijöidemme oikeudet ja yksityisyyden mahdollisilta tietosuojaloukkauksilta.

8. Riskienhallinta

Pysymme tietoisina yhtiömme ja lainsäädännön nykytilasta, ja mukautamme tietosuojakäytäntöjämme aina tilanteen vaatiessa. Näin hallitsemme yhtiöömme kohdistuvat tietosuojariskit ja kykenemme minimoimaan ne ajoissa.